

It is the policy of the UNC Health Care and its affiliated Network Entities (individually and collectively called "UNC HC" herein) that users (i.e., employees, medical staff, students, volunteers, vendors, outside affiliates, and any others who are permitted access) shall respect and preserve the privacy, confidentiality, and security of confidential information ("CI" In the course of providing services for or at UNC HC, I may encounter these types of CI: (1) patient information (such as medical records, billing records, and conversations about patients), (2) personnel information (payroll, discipline, or other information about employees, volunteers, students, contractors, or medical staff), (3) confidential business information of UNC HC, its affiliated Network Entities, and/or third parties, including third-party software and other licensed products or processes, or (4) operations, quality improvement, peer review, education, billing, reimbursement, administration, or research (such as utilization reports, survey results, and related presentations. This information from any source and in any form, including, but not limited to, paper record, oral communication, audio recording, and electronic display, is strictly confidential. I understand and agree that I will only access, maintain, use or disclose CI on a legitimate job-related, need-to-know basis, and that I will limit my access, maintenance, use or disclosure of CI to the minimum amount of CI necessary to accomplish the intended purpose of the use, disclosure, or request. I further agree that:

- 1) I will protect the privacy, confidentiality, and security of UNC HC patient information, including electronic health records ("EHR"), in accordance with federal and state regulations and applicable policies and procedures.
- 2) I will complete all required privacy and security training for accessing EHR or other CI.
- 3) I will not maintain CI on a mobile device (laptop, smartphone, tablet, etc. that is not encrypted and will not electronically transmit CI in an unsecured manner or to an unencrypted mobile device.
- 4) I will not disclose to another person my sign-on code and/or password, and I will not use another person's information, for accessing EHR or other CI. I will not leave a secured application unattended while I am signed on.
- 5) I will not attempt to access a secured application or restricted area without proper authorization or for purposes other than official UNC HC business.
- 6) I will not alter or destroy unless alteration or destruction is part of my job or services for UNC HC, in which case I will not only alter or destroy CI in accordance with applicable policies and procedures.
- 7) I will immediately report to my supervisor any known or suspected (a) use of my password by someone other than me, or (b) inappropriate access, use or disclosure of CI.
- 8) I will safeguard from loss, theft, or unauthorized use/access UNC HC owned equipment/property on which CI is stored or through which CI may be accessed.
- 9) I will not store or transmit CI via my personal equipment/property unless permitted by and in accordance with applicable policy or procedure.
- 10) I will not post or discuss CI of any type to social media sites unless pre-approved by UNC HC.
- 11) I will not take photographs, make videos, or make other recordings of patients, staff, or visitors except in accordance with applicable UNC HC policies and procedures.
- 12) I understand that my access to CI and my UNC HC email account may be audited.
- 13) I will not access or obtain my own, a friend's, or a family member's patient information maintained by UNC HC without appropriate written authorization and under applicable policies and procedures.